Department of Homeland Security
Information Analysis and Infrastructure Protection
Daily Open Source Infrastructure Report for 08 October 2003

Current Nationwide Threat Level is
ELEVATED
Significant Risk of Terrorist Attacks
For info click here
www.whitehouse.gov/homeland

Daily Overview

- The Register reports a successful terrorist attack on America's financial infrastructure − key nodes Fedwire and Fednet − could bring the U.S. and global economies to a standstill. (See item 6)
- The Associated Press reports for three years, a student attending Mesa Community College in Arizona, allegedly used more than 50 identities − stolen from inmates serving long sentences − to secure more than $300,000 in student loans. (See item 7)
- The Washington Post reports Maryland, Washington, DC, and Virginia cases of Legionnaires' disease have more than tripled in the past nine months and caused at least nine deaths. (See item 16)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *October 08, Agence France−Presse* — **Major power failure blacks out Czech Republic.** Tens of thousands of people were left without electricity in a major power failure in western parts of the Czech Republic on Monday, October 6, a spokesperson for the local supplier ZSE said. **"We are investigating the reasons for the power failure and the losses suffered as a result," spokesperson Miroslav Kucera said. The blackout brought down the hydraulic**

power plant at Karlovy Vary, a town with 60,000 inhabitants. Kucera said it cut the electricity supply to the cities of Ostrov, Nejdek, Rotava, and all the smaller towns in between. He says the blackout occurred at 11:00 p.m. local time and power was restored about half an hour later. There have, in recent weeks, been several big power blackouts in the United States, Canada, Britain, Italy, Denmark and Sweden.
Source: http://www.abc.net.au/news/justin/weekly/newsnat−8oct2003−7. htm

2. *October 07, Expatica (Netherlands)* — **Nuclear materials regularly intercepted.** Terrorist attempts to smuggle raw materials destined for the foreign production of nuclear weapons are thwarted several times in the Netherlands each year, the Dutch secret service AIVD has revealed. Fears of nuclear attacks using "dirty bombs" or stolen nuclear equipment increased dramatically after the September 11 terrorist attacks in the U.S. in 2001. **The Dutch secret service has since warned universities and businesses in the Netherlands to be on extra alert for suspicious people. It warned that terrorists are not only aiming to export raw materials, but are increasingly trying to gather knowledge.** This means that nuclear weapons could theoretically be produced in the Netherlands. To minimize the potential risk, the AIVD has drawn up a checklist so that businesses and universities can individually determine which people or businesses represent a threat. **It warned organizations to be watchful of individuals or companies not interested in after−sales service and maintenance, requesting different packaging, or ordering an amount that differs from normal civil uses.** The AIVD also said terrorists presents themselves to western universities as students or researchers wishing to obtain information, confirming that the Internet is also used to establish contact.
Source: http://www.expatica.com/index.asp?pad=2,18,&item_id=34776

[Return to top]

Chemical Sector

3. *October 06, News 12 (Long Island)* — **Chemical fire at a Long Island park last weekend causes concern.** A chemical fire at a Franklin Square park last weekend is raising questions about some Hempstead Town parks. **On Saturday, Rath Park in Franklin Square had to be evacuated as a Hazmat team cleaned up a 55−gallon drum of pesticides that spontaneously ignited. The Town of Hempstead collects hazardous household materials at town parks as part of the STOP (Stop Throwing Out Pollutants) Program.** The program is run in eight locations, all of them in parks. Some town residents say bringing hazardous materials to a place where kids play nearby does not make sense. Town officials argue that they intentionally chose dumpsters in parks for the STOP program because they are safe and well isolated.
Source: http://www.news12.com/LI/topstories/article?id=91914

[Return to top]

Defense Industrial Base Sector

4.

October 07, New York Times — **Rapid reaction force exercise to be included in NATO meeting.** NATO's defense ministers and military chiefs arrived in Colorado Springs, CO, on Tuesday, October 7, to study how the alliance's proposed rapid reaction force might be deployed in a crisis. A senior Defense Department official said the meeting would be the first time that NATO's top military and civilian defense officials would join in a rapid reaction force exercise, which the Pentagon was studiously describing as a "study seminar" and not a war game. **One senior Pentagon official said the goal was to "illuminate some of the issues that will arise from the creation" of the NATO Response Force. The force is scheduled to go into service next summer and be fully operational in 2006.** Plans call for the alliance to be able to deploy a brigade − usually a military unit of about 5,000 members − within 5 to 30 days, the official said. But to sustain that level of readiness around the clock, along with the required air and naval complement, could require a commitment of 15,000 to 20,000 members of NATO military services. The force would be the alliance's first standing military contingent, able to rush to a crisis within Europe or beyond.
Source: http://www.nytimes.com/2003/10/07/international/americas/07NATO.html

5. *October 06, CNN* — **Pentagon sold biolab gear according to GAO.** The Department of Defense (DoD) sold equipment to the public that can be used for making biological warfare agents, according to a draft report by the General Accounting Office (GAO). The DoD agency responsible for the sale of excess property to the public, the Defense Reutilization and Marketing Service, halted the sale of such items September 19 while the practice is reviewed. **"Many items needed to establish a laboratory for making biological warfare agents were being sold on the Internet to the public from DoD's excess property inventory for pennies on the dollar, making them both easy and economical to obtain," the GAO draft report said.** Much if not all of the equipment sold to GAO investigators is available to the public at full price on the open market, the source said, but "we certainly don't need DoD to be a discount shop for potential bioterrorists." The source conceded that "only nominal controls" are now in place to prevent the sale of such items to the public."
Source: http://www.cnn.com/2003/US/10/06/gao.pentagon/index.html

[Return to top]

Banking and Finance Sector

6. *October 07, The Register (UK)* — **Expect terrorist attacks on global financial system.** A successful terrorist attack on America's financial infrastructure could bring the U.S. and global economies to a standstill, and the real surprise is that it hasn't been attempted yet. **"We've gone after al Qaeda's finances, and it would strike me that in a sense, we can expect retaliation in kind," said Phil Williams,** Director of the Program on Terrorism and Trans−National Crime at the University of Pittsburgh. At the annual conference of the Center for Conflict Studies, **Williams says the attack, when and if it comes, would likely focus on what he calls key nodes in the U.S. financial infrastructure: Fedwire and Fednet.** Fedwire is the financial funds transfer system that exchanges money among U.S. banks, while Fednet is the electronic network that handles the transactions. The system has one primary installation and three backups. "You can find out on the Internet where the backups are. If those could be taken out by a mix of cyber and physical activities, the U.S. economy would basically come to a halt," Williams said. If the takedown were to include the international funds transfer networks CHIPS

and SWIFT then the entire global economy could be thrown into chaos.
Source: http://www.theregister.co.uk/content/55/33269.html

7. *October 02, Associated Press* — **Man used stolen IDs to scam student loans. For three years, John Edward Christensen attended Mesa Community College in Arizona, where he allegedly used more than 50 identities − stolen from inmates serving long sentences − to secure more than $300,000 in student loans.** Authorities said they suspect Christensen used some of the money to buy a house and a car. A federal grand jury has indicted the 62−year−old on four counts of theft and fraud involving about $313,000 in student financial aid. The indictment also seeks the forfeiture of more than $58,000 from 10 bank accounts and about $11,000 found during searches of Christensen's home and car. He was arrested September 2. According to the indictment, campus and Mesa police arrested Christensen at Mesa Community College after he tried to claim a financial aid check. Christensen had three fake identifications in his possession when he was arrested, officials said.
Source: http://www.azcentral.com/news/articles/1002StolenIDs02−ON.ht ml

[Return to top]

Transportation Sector

8. *October 07, Associated Press* — **Man allegedly had dagger in New Jersey airport. A man trying to board a Los Angeles−bound flight was arrested after an eight−inch dagger was found inside one of his shoes, officials said.** Vincent P. Rosso was stopped Monday at Newark Liberty International Airport when a federal screener told his supervisor that Rosso appeared to be concealing a dagger in either his coat or sneakers. **The dagger was detected when the items went through an X−ray machine, said Tony Ciavolella, a Port Authority spokesman. The weapon was found in a cavity in the sole of Rosso's left sneaker during a subsequent hand inspection.** Rosso, 25, was charged with unlawful possession of a weapon. He posted $10,000 bail and was released. Officials do not believe Rosso has any terrorist links, but the FBI is reviewing the case.
Source: http://www.nytimes.com/aponline/national/07WIRE−AIRPORT.html

9. *October 07, Miami Herald* — **Engine explodes on charter plane, forcing a return to Miami. An engine exploded on a Swiss charter airline Sunday morning shortly after it took off from Miami International Airport with 175 people aboard. Edelweiss Air Flight No. 565 en route to Zurich returned to the airport and no injuries were reported,** said Lauren Peduzzi, spokesperson for the National Transportation Security Board, which is investigating the incident. **However, the explosion of the Rolls−Royce engine damaged the Airbus A330's wing, and pieces of the engine could have penetrated the passenger cabin.** The twin−engine Airbus A330 departed Miami at 1:28 a.m. and returned at 2:11 a.m., said Marc Henderson, Miami International Airport spokesman. The plane's left engine failed no more than 40 miles outside the airport, he said. Edelweiss' charter flight has flown nonstop to Zurich on Sunday mornings since July 5. Peduzzi said the aircraft is still in Miami, and Rolls−Royce is making arrangements to remove the engine and ferry it to Derby, England, to analyze it. **Engine explosions are unusual, and the flying metal can kill passengers.** In 1996, a Pratt & Whitney JT8D−219 engine on a Delta MD−88 failed as the plane took off from Pensacola. Debris tore into the plane's cabin, killing a Michigan woman and her 12−year−old son.

Source: http://www.miami.com/mld/miamiherald/6955792.htm

10. *October 07, Associated Press* — **Deadly train crash renews call for new technology.** A collision of trains in California last year that killed three people and injured dozens was caused by a freight crew's failure to heed a signal, federal safety officials said Tuesday. **The National Transportation Safety Board (NTSB) reiterated its call for the rail industry to come up with crash−avoidance technology, something the NTSB has pushed since 1990. Federal Railroad Administration spokesman Warren Flatau said the agency planned to issue standards for such systems later this year.** "We believe it is going to greatly enable and accelerate the pace at which railroads proceed in further developing or installing these types of systems," said Flatau, whose agency has spent more than $66 million on developing the technology. **The FRA and the railroad industry have been testing crash−avoidance technology in recent years.** The Burlington Northern Santa Fe announced in July that it was installing and testing technology along a 135−mile stretch of track in Illinois. **The test uses the global positioning system to let the train engineer know, through a computer screen mounted in the locomotive, of any hazards along the tracks. If the engineer fails to respond, the computer automatically stops the train.**
Source: http://www.bayarea.com/mld/mercurynews/news/local/6955834.ht m

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

11. *October 07, USAgNet* — **Compliance almost total on FDA rule. Companies subject to the Food and Drug Administration's (FDA) ruminant feed rule to prevent bovine spongiform encephalopathy (BSE) in the United States have a nearly 100% compliance rate**, according to an update published this week by the FDA's Center for Veterinary Medicine. Of the 1,664 inspected firms handling prohibited materials, six firms, fewer than 1%, had official action taken against them. **Only 171 firms were classified as voluntary action indicated (VAI)**, which means inspectors found conditions of little regulatory significance yet still warranting correction. FDA currently inspects 11,375 firms, only 15% of which are handling prohibited materials. The data were assembled from inspections conducted and reported by September 23.
Source: http://www.usagnet.com/story−national.cfm?Id=1080&yr=2003

12. *October 06, Reuters* — **Japan's mad cow case may affect U.S.−Canada trade. The U.S. Department of Agriculture (USDA) said Monday, October 6, it was seeking more details about a new case of mad cow disease in a young animal in Japan, which could impact a USDA plan to reopen U.S. borders to shipments of live Canadian cattle that are under 30 months of age**. Japanese officials earlier confirmed the case of mad cow disease, the eighth since the illness was discovered in September 2001. It was the first confirmed case in Japan in a cow less than two years old. Japan, the largest buyer of U.S. beef, has required all American

beef shipments be certified Canadian−free after Canada reported its first case of mad cow disease in May. The U.S. has never reported a case of mad cow disease. **The 30−month age limit was established after studies showed mad cow disease does not develop in animals that young**. The United States has begun allowing some "low−risk" beef products derived from young cattle, but continues to ban live imports. A USDA proposal to allow live Canadian cattle was expected within weeks.
Source: http://story.news.yahoo.com/news?tmpl=story&cid=571&ncid=751&e=4&u=/nm/20031006/hl_nm/health_madcow_usa_dc

[Return to top]

Food Sector

13. *October 07, Pacific Business News* — **World relies more heavily on fish for food.** China, the world's most populous nation, consumes more than a third of the world's fish harvest. Its consumption has tripled in 24 years. **The International Food Policy Research Institute, says world fish demand, now about 100 million tons a year, will soar to 128 million tons by 2020**. Developing nations in general seem to be using a lot more fish as their populations rapidly grow. Industrial nations' share of fish consumption, by contrast, shrank from 55 percent in 1973 to 31 percent in 1997. The institute predicts that world aquaculture production, now about 30 million tons a year, will top 50 million tons in a decade or so. By 2020 fish farms will meet 40 percent of world fish demand, the institute predicts.
Source: http://pacific.bizjournals.com/pacific/stories/2003/10/06/da ily16.html

[Return to top]

Water Sector

14. *October 07, OrlandoSentinel.com* — **Orange, Lake challenge huge OUC water deal. Florida's Lake and Orange counties Monday fired what could be the first shot in a long−predicted Central Florida water war, directly challenging the Orlando Utilities Commission's (OUC) right to pump billions of gallons of water a year from the underground aquifer.** The regional showdown over how to divide a dwindling drinking−water supply goes to the heart of key environmental and growth challenges that could embroil the state for decades. The outcome could affect everything from how fast cities can grow to how much customers pay for water. **The dispute centers on a pending 20−year permit that the Orlando Utilities Commission negotiated with the St. Johns River Water Management District, which controls the use of most of Central Florida's water.** Orange County Utilities Department officials, who provide water to more than 62,000 customers in unincorporated areas and Windermere, decided Monday to join Lake in challenging OUC's arrangement. **Lake County commissioners contend the deal would harm the underground water supply that is the source of 90 percent of the state's drinking water.** "It's such a tremendous amount of water," said Lake County attorney Sandy Minkoff. "It would have a serious detrimental effect on the county's resources."
Source: http://www.orlandosentinel.com/news/local/orl−asecwater07100703oct07,0,3299818.story?coll=orl−news−headlines

[Return to top]

Public Health Sector

15. *October 07, Associated Press* — **Cancer myth often prevents surgery. Thirty−eight percent of patients who responded to a survey in five urban clinics believed the myth that cancer spreads when exposed to air during surgery.** Doctors administered a voluntary and anonymous questionnaire to 626 patients at clinics specializing in lung diseases and lung tumors. The questionnaire was given at five urban outpatient facilities between 1999 and 2000. Of the 38 percent who said they believed that cancer spreads when exposed to air, 24 percent said they would reject lung cancer surgery based on that belief. Nineteen percent said they would reject surgery even if their doctor told them the belief had no scientific basis. Mitchell Margolis, director of clinical medicine at the Philadelphia Veterans Affairs Medical Center, who said he got the idea for the survey after hearing the myth repeated by a "disconcerting number" of patients, said the respondents were largely middle−aged and elderly men. **"The overall message here is the importance of cultural sensitivity among health care providers in general, a greater awareness of what people's fears are, and being able to listen for them,"** said Alfred Munzer, a lung specialist at Washington Adventist Hospital in Takoma Park, MD.
Source: http://www.cbsnews.com/stories/2003/10/07/health/main576883. shtml

16. *October 07, Washington Post* — **Washington area officials investigate spike in Legionnaires' cases. Maryland, Washington, DC, and Virginia cases of Legionnaires' disease have more than tripled in the past nine months and caused at least nine deaths, leaving health officials mystified and concerned.** By mid−September, the three jurisdictions had reported 178 cases of the pneumonia−like illness so far this year, compared with 48 at the same point last year. **However, the newest cases aren't following the usual pattern, in which outbreaks have been tied to a specific water source, such as a hotel air conditioning system, a whirlpool spa, a hospital's water systems or even a grocery store mister.** Instead, most appear to be cases in which individuals contracted the disease from the water in their home, workplace or neighborhood, but others around them did not. **The area's heavy rains may have favored the growth of Legionella bacteria in bodies of fresh water as well as water systems and damp environments,** said Daniel Feikin, medical epidemiologist at the CDC, but exactly how the extra rain may have allowed more of the bacteria into potable water, he can't explain.
Source: http://www.washingtonpost.com/wp−dyn/articles/A53100−2003Oct 6.html

17. *October 06, Center for Infectious Disease Research & Policy* — **Smallpox vaccine−heart attack link unlikely, historical study suggests. New York City health records show no increase in cardiac deaths after a citywide smallpox vaccination campaign in 1947, which supports the view that cardiac events in 16 people vaccinated recently were unrelated to the vaccine, according to the Centers for Disease Control and Prevention (CDC).** The records were examined as part of the investigation triggered by ischemic cardiac events in the 16 military and civilian vaccinees, three of whom died, according to the October 3 issue of Morbidity and Mortality Weekly Report. The three people who died−two civilians and one military man−were all in their mid−50s and had several risk factors for heart disease. The

deaths occurred between four and 17 days after vaccination. **In the current immunization program involving military personnel and selected civilian health workers, the CDC uses screening guidelines designed to minimize cardiac risks by excluding people with heart disease or three or more cardiac risk factors.** That precaution should be maintained even though this study casts doubt on the possible link between smallpox vaccine and fatal cardiac events, the report says. Report: http://www.cdc.gov/mmwr/preview/mmwrhtml/mm5239a1.htm Source: http://www.cidrap.umn.edu/cidrap/content/bt/smallpox/news/oc t0603smallpox.html

[Return to top]

Government Sector

18. *October 07, New York Times* — **Department of Homeland Security plans overseas offices.** The Department of Homeland Security (DHS) plans to open law enforcement offices throughout the Muslim world, with agents assigned to investigate visa applicants who are suspected of ties to al Qaeda and other terrorist groups, senior Bush administration officials said on Monday. **The officials said permanent offices would open early next year in American embassies and consulates in Egypt, Indonesia, Morocco, Pakistan and the United Arab Emirates, chosen because of their visa volume and because of the regional presence of al Qaeda and other terrorist groups.** Two offices opened in August without announcement in Saudi Arabia, one in Riyadh, the capital, and the other in Jeddah, the commercial center. American officials said opening the offices reflected a major expansion of the efforts to scrutinize visa applications, particularly from regions where terrorist groups operate. Source: http://www.nytimes.com/2003/10/07/politics/07TERR.html

[Return to top]

Emergency Services Sector

19. *October 07, Associated Press* — **Schools to get federal tools to help with bomb threats.** School districts and public safety agencies across the nation will receive a new package of tools to help handle school bomb threats, federal officials announced Tuesday. **The centerpiece of the effort is a compact disc with information about such topics as preventing and planning for bomb threats, providing training to staff and responding to explosions.** The Bureau of Alcohol, Tobacco, Firearms and Explosives and the Education Department are partners in the project. "Unfortunately, we know it is almost inevitable that schools will receive bomb threats and will need a plan for dealing with them," said ATF Acting Director Bradley Buckles. **Even when no bombs are found, as is usually the case, threats cause a climate of fear and force schools to contend with lost class time, the ATF says.**
Source: http://www.cnn.com/2003/EDUCATION/10/07/bomb.threats.ap/inde x.html

20. *October 07, Iowa City Press−Citizen* — **Federal program to test skills of local responders.** While the test will be real, the event is pretend − an elaborate training exercise, in Iowa City, IA. **The federally−sponsored program is designed to assess nationwide capability for these types of incidents, said Tim Bell, a member of the emergency response team for the event's host, Procter & Gamble.** The southeast Iowa City plant produces shampoo,

conditioner and mouthwash. Participants include local police, fire and medical responders. Bell said he cannot discuss the chemical responders would be tested on during the outdoor event, but said there are several plans to handle different chemicals. Iowa City Fire Chief Andy Rocca said the assessment would allow firefighters to work through a drill in a controlled situation and assess their capabilities. **The program is called CHER−CAP, for Comprehen−sive HAZMAT Emergency Response−Capability Assessment Program. It focuses on issues specific to HAZMAT preparedness and response by drawing together public and private sectors at the local level, according to the Federal Emergency Management Agency.**
Source: http://www.press−citizen.com/news/100703drill.htm

21. *October 07, Washington Post* — **Ruptured gas main causes Washington, DC hospital evacuation. A gas main near George Washington University Hospital ruptured this morning, starting a fire along a stretch of street that forced the evacuation of the emergency room and some operating rooms.** No serious injuries were reported, and authorities said they capped the leak within about 30 minutes. **It was unclear exactly when the line began leaking gas, but District Fire Chief Adrian H. Thompson said that officials believe that the line could have been damaged somehow in the nearby demolition work.** Officials said that the gas might have been ignited after a car on 23rd Street hit a pothole, emitting a spark. **That triggered flames that at one point rose 20 feet high and covered a stretch of 23rd Street near Washington Circle.** Thompson said that the way the fire started could have been a "blessing in disguise" because it appeared to happen before a great deal of gas escaped. **Shortly after the fire began, hospital officials quickly took precautions even though the building itself never caught fire. They moved people from the emergency and operating rooms, in the northern side of the building, to other parts of the hospital that were deemed safer.** Dr. John Williams, provost and vice president of health affairs, said that the emergency procedures went smoothly.
Source: http://www.washingtonpost.com/wp−dyn/articles/A55575−2003Oct 7.html

[Return to top]

Information and Telecommunications Sector

22. *October 07, Reuters* — **Virus writers probed for terror ties. The National Hi−Tech Crime Unit (NHTCU), Britain's task force against high−tech crime, has started working to identify patterns in the source code of the most damaging Internet worms and virus programs to determine whether they are the work of organized subversive groups or crime syndicates**. The hope is that buried somewhere in the lines of code will be clues to the author's identity, motive and possibly, future acts of sabotage. A mounting concern is that a program could bore into a computer network and compromise, say, a police emergency response phone system or air traffic control system. **A digital attack in isolation would inflict relatively little damage, but should the incident be timed to coincide with a physical act of sabotage the toll could be high**. In the wake of the September 11, 2001 attacks in the United States, response plans to all potential acts of sabotage−−digital or physical−−are being reviewed. Detective Chief Superintendent Len Hynds, head of the NHTCU, said the NHTCU has trained officers to work with the UK's National Infrastructure Security Coordination Center, the government body charged with protecting critical infrastructure, in honing a response.
Source: http://www.washingtonpost.com/wp−dyn/articles/A54868−2003Oct 7.html

23. *October 06, Computerworld* — **DHS launches cybersecurity monitoring project.** The Department of Homeland Security's (DHS) cybersecurity division creating a real−time cybersituation−awareness system, a senior DHS official said this week. **The aim of the system is to provide a nationwide capability to conduct instant analysis of security incident data for signs of coordinated attacks or major virus and worm outbreaks**. Sallie McDonald said the National Cyber Security Division of the DHS is developing a nonproprietary data collection system that will run on an automated security extranet and feed incident reports to the various Information Sharing and Analysis Centers (ISACs) operating in the private sector. The ISACs would then feed the data to the national situation−awareness system. **The new incident reporting and analysis system will be launched in December** at the first DHS−sponsored Cyber Security Summit to be held in Silicon Valley, said McDonald. The DHS also plans to announce a security awareness effort targeted at 50 million home users and small businesses, and will draft a national cybersecurity road map that includes specific milestones and metrics for measuring progress in bolstering security.
Source: http://www.pcworld.com/news/article/0,aid,112764,00.asp

24. *October 06, Star Tribune (Minneapolis)* — **Feds take up arms as computer crime becomes multibillion−dollar problem.** The Minnesota Cyber Crimes Task Force will be in operation by the end of the year. **The task force will be the first office in the nation to combine the efforts of the FBI, Secret Service and the U.S. attorney's office**. Paul McCabe, a special agent in the Minneapolis FBI office, said **it will investigate crimes that include Internet attacks, online fraud, cyberspace theft of intellectual property, online child pornography and the use of the Internet as a communications medium for terrorists**. Paul Luehr, an assistant U.S. attorney who prosecutes many of the federal cyber crime cases in Minnesota, said the task force promises a new way of handling cyber crimes because in the past the two federal investigative agencies have tended to go their own way, with the Secret Service heading up cyber crime investigations in New York and San Francisco and the FBI running comparable investigations in Pittsburgh and San Diego. McCabe said the FBI will contribute 10 people, including seven investigators and three "computer forensic examiners" who examine seized computers for evidence and know their way around the Internet.
Source: http://www.startribune.com/stories/789/4137187.html

25. *October 06, Associated Press* — **Iraq awards mobile telephone contracts.** Iraq's reconstruction got a boost Monday, October 6, when licenses were awarded for wireless phone networks that are expected to be operating within weeks in a country bypassed by the cellular revolution. The licenses were awarded to three Middle Eastern companies that have investors in Iraq and elsewhere in the region. "This is an important day for Iraq," said Communications Minister Haider Jawad al−Aubadi. **"Iraq badly needs the mobile system to enhance the security of the country." The mobile system will especially help in Baghdad, where 12 landline telephone exchanges were knocked out during the U.S.−led invasion last spring. Nationwide, one in four phone lines remains out of service**. Before the war, Iraq had just three phone lines for every 100 people. The wireless buildup will bring hundreds of millions of foreign dollars into Iraq, where continuing guerrilla violence against U.S.−led occupation forces could delay major redevelopment investment. **The companies all operate with the GSM phone standard** widely used in Europe and the Middle East.
Source: http://www.washingtonpost.com/wp−dyn/articles/A52475−2003Oct

6.html?referrer=email

26. *October 06, BBC* — **Hacker attack left port in chaos .** Aaron Caffrey, 19, allegedly hacked into the computer server at the Port of Houston in Texas on September 20, 2001 in order to target a female chatroom user following an argument, a UK court has heard. It was claimed that the teenager intended to take the woman's computer offline by bombarding it with a huge amount of useless data, and he needed to use a number of other servers to be able to do so. Prosecutor Paul Addison told the court that the attack bombarded scheduling computer systems at the world's eighth largest port with thousands of electronic messages. **The port's Web service, which contained crucial data for shipping pilots, mooring companies and support firms responsible for helping ships navigate in and out of the harbour, was left inaccessible. It is thought to be the first time that part of a country's national infrastructure has been disabled by an electronic attack**. Addison said: "The data on the server contains information on navigation, tides, water depths and weather. No injury or damage was, in fact, caused." Following an investigation, American authorities were able to trace the computer's internet provider number to a computer at Caffrey's home. He was arrested and questioned by police in January 2002.
Source: http://news.bbc.co.uk/1/hi/england/hampshire/dorset/3168696. stm

Internet Alert Dashboard

Current Alert Levels

AlertCon: 1 out of 4 https://gtoc.iss.net	Security Focus ThreatCon: 1 out of 4 http://analyzer.securityfocus.com/

Current Virus and Port Attacks

Virus:	#1 Virus in the United States: **WORM_LOVGATE.G** Source: http://wtc.trendmicro.com/wtc/wmap.html, Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	135 (epmap), 80 (www), 137 (netbios−ns), 1434 (ms−sql−m), 445 (microsoft−ds), 1433 (ms−sql−s), 139 (netbios−ssn), 25 (smtp), 4662 (eDonkey2000), 27374 (SubSeven) Source: http://isc.incidents.org/top10.html; Internet Storm Center

[Return to top]

General Sector

27. *October 07, Associated Press* — **Projectile fired at Iraqi Foreign Ministry.** A projectile was fired Tuesday, October 7, at the offices of the Iraqi Foreign Ministry, causing a large explosion but no casualties, witnesses said. Iraqi guards fired rifles in the air shortly after the midmorning blast. Five U.S. Army Humvees and two armored personnel carriers sped to the scene in

western Baghdad, and several streets in the area were sealed off. **The projectile, which apparently exploded in the ministry compound, caused minimal damage but sent employees streaming out of the offices, located about a half mile from the palace headquarters of the U.S.−led coalition. The ministry is also about a half mile from the Al−Rasheed Hotel, where many U.S. officials live**. The hotel was attacked by small rockets or rocket−propelled grenades on Sept. 27, causing no casualties and minimal damage.
Source: http://www.foxnews.com/story/0,2933,99308,00.html

[Return to top]

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web−site (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings − DHS/IAIP Assessements, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications − DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

DHS/IAIP Daily Reports Archive − Access past DHS/IAIP Daily Open Source Infrastructure Reports

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703−883−6631
Subscription and Distribution Information	Send mail to nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703−883−6631 for more information.

Contact DHS/IAIP

To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at nipc.watch@fbi.gov or call 202−323−3204.

DHS/IAIP Disclaimer